WEB APPLICATION FIREWALL

FortiWeb Release Notes

VERSION 6.0.1

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

September 4, 2018

FortiWeb 6.0.1 Release Notes

2nd Edition

Change log

08/24/2018	Initial release.
09/04/2018	Added 0480895 to *Resolved Issues*. Added 0511242 to *Known Issues*.

TABLE OF CONTENTS

Introduction

FortiWeb is a web application firewall (WAF) that protects hosted web applications from attacks that target known and unknown exploits. Using multi-layered and correlated detection methods, FortiWeb defends applications from known vulnerabilities and zero-day threats. The Web Application Security Service from FortiGuard Labs uses information based on the latest application vulnerabilities, bots, suspicious URL and data patterns, and specialized heuristic detection engines to keep your applications safe.

FortiWeb also offers a machine-learning function that enables it to automatically detect malicious web traffic. In addition to detecting known attacks, th feature can detect potential unknown zero-day attacks to provide real-time protection for web servers.

FortiWeb allows you to configure these features:

- Vulnerability scanning and patching
- IP reputation, web application attack signatures, credential stuffing defense, anti-virus, and FortiSandbox Cloud powered by FortiGuard
- Real-time attack insights and reporting with advanced visual analytics tools
- Integration with FortiGate and FortiSandbox for ATP detection
- Behavioral attack detection
- Advanced false positive and negative detection avoidance

FortiWeb hardware and virtual machine platforms are available for medium and large enterprises, as well as for service providers.

For additional documentation, please visit the FortiWeb documentation:

http://docs.fortinet.com/fortiweb/

What's new

FortiWeb 6.0.1 offers the following new feature and enhancements.

New features

New FortiWeb platform—FortiWeb Container

FortiWeb can now run as a container on the Docker container platform. The new solution allows you to easily provision FortiWeb into your microservice's architecture and use it as a cloud-native, DevOps enabled, and containerized WAF.

Add Parameter View in Machine Learning Policy

Parameter View tab is added in **Machine Learning** > **Machine Learning Policy**. It displays probability boxplots, Anomalies triggered by HMM, and other informations related with parameters.

For more information on Parameter View, see View domain data section in *FortiWeb 6.0.1 Administration Guide*.

Enhance Tree View tab in Machine Learning Policy

The **Parameter** table in **Machine Learning** > **Machine Learning Policy** > **Tree View** displays the machine learning status. It shows the percentage of the samples collected and the progress of the model testing.

Rebuild entire URL path directory in Machine Learning Policy

In 6.0, you can only rebuild machine learning models for URLs. In 6.0.1, it is now possible to rebuild an entire URL directory. This means you can select a specific URL directory, and click **Rebuild Directory** to rebuild machine learning models for all the sub-URLs under the selected URL directory.

Support exporting and importing machine learning data

Under the **Machine Learning** section of **Policy > Server Policy**, or the **Allow sample collection for Domains** section of **Machine Learning > Machine Learning Policy**, you can export the data generated by the machine learning policy, or import the machine learning data from your local directory to FortiWeb.

New Sample Collection mode in Machine Learning Policy

Two sample collection modes are supported: **Normal** and **Fast**. In Normal mode, up to 5000 samples will be collected for building a machine learning model. In Fast mode, at most 2500 samples will be collected. The default sample collection mode is Normal.

Add logs to record FortiWeb internal performance information

FortiWeb now supports downloading internal performance information from **System** > **Maintenance** > **Debug** > **Download**. It records logs for flow, dmesg, top, perf, etc.

Support Java Unicode decoding

FortiWeb now supports Java Unicode decoding for parsing protocols.

Add multiple categories in Server Policies tab

In addition to listing the CVE IDs of the policy violations, **Server Policies** tab now supports more categories including **Threats**, **Sources**, **Countries**, **Client Devices**, **HTTP Methods**, and **URLs**.

For more information on Server Policies tab, see Server Policies section in *FortiWeb 6.0.1 Administrator's Guide*.

Add CVE ID in Countries tab and Threats tab

CVE ID category is added in **FortiView** > **Security** > **Countries** and **FortiView** > **Security** >**Threats**.

Support HTTP PATCH method

HTTP parser now supports the HTTP PATCH method. It is added in Allow Method, Machine Learning, Signatures, and Auto Learn.

Support SPNEGO Kerberos

SPNEGO Kerberos is now supported in Site Publish. SPNEGO and KRB5 are two kinds of authorization mechanism. They are used by web servers to retrieve Kerberos tickets. Before 6.0.1 release, FortiWeb only supports KRB5 mechanism. Now SPNEGO can also be configured if you choose Kerberos delegation in Site Publish Rule (**Application Delivery** > **Site Publish** > **Site Publish** > **Site Publish Rule**).

Support WSDL verification

Web Services Description Language (WSDL) verification is added to **XML Protection**. FortiWeb can verify the legality of the WSDL file, and check the SOAP message against WSDL and SOAP protocol if the Data Format in a XML Protection rule is selected as **SOAP**.

Add FortiSandbox cloud connectivity status

The connectivity status of FortiSandbox cloud is displayed on the FortiSandbox page and FortiGuard's dashboard widget.

Feature enhancements

Add more action settings in Machine Learning Policy

Except from setting alert or deny actions for the anomalies detected by machine learning policies, now you can also set the period block, severity level and trigger actions for the anomalies.

Support wildcard * in Machine Learning Domain Name

In the **Allow Sample Collection for Domains** section of **Machine Learning Profile**, wildcard * is supported to cover multiple domains, so that samples can be collected for multiple domains in one profile.

Add X-Forwarded-For support for sample collection in Machine Learning Policy

If **Server Objects** > **X-Forwarded-For** is set and referred in Web Protection Profile, the machine learning policy will check against the X-Forwarded-For policy configuration to record the source IP of the samples.

Add sample collection limit for each IP address in Machine Learning Policy

Sample collection limit is added by default for each IP address. The default value is 30, which means at most 30 samples can be collected from each IP address. You can change it to a value that you desire through CLI. You can also remove the limit by setting the value to 0.

If you have set **Allow Sample Collection from IPs**, the sample collection limit will not take effect, which means FortiWeb will not limit the number of samples collected from the specified IP ranges.

Support NTP IPv6 address

FortiWeb now supports synchronizing with NTP servers with IPv6 address (**System** > **Maintenance** > **System Time** > **Synchronize with NTP server**).

Add CLI commands for Config-Synchronization

You can now run CLI commands to execute Config-Synchronization.

```
execute conf_sync push
execute conf_sync test
```

Change and performance notices

Machine learning data is deleted when upgraded to 6.0.1

If you upgrade from 6.0 to 6.0.1 , or downgrade from 6.0.1 to 6.0, the machine learning data will be cleared, but the machine learning configurations will be kept as is.

Remove Data Analytics

Since FortiView is in use and can fully replace the functions of Data Analytics, this feature is removed in 6.0.1.

Remove fast forward mode

Fast forward mode is no longer supported in FortiWeb. It's removed from all related features.

Recursive URL Decoding is Enabled by default

The Recursive URL Decoding option (**System** > **Config** > **Advanced**) is enabled by default.

Machine learning policy violations are reclassified in FortiView

Before 6.0.1, in the threat list table in **FortiView** > **Security** > **Threats**, the machine learning policy violations are listed separately from other threat types. Starting from 6.0.1, machine learning policy violations will no longer be listed separately. They are reclassified into corresponding threat types such as **Known Exploits**, **SQL Injection (Extended)**, etc.

Add limits for HA EtherType

Two restrictions are added for HA EtherType (`Config System HA`).

- It's only allowed to use numbers between 0x8890–0x889f (inclusive) as HA EtherType.
- The numbers for different HA EtherTypes can't be the same.

Events of the virtual interfaces will no longer be monitored

For releases earlier than 6.0.1, FortiWeb monitors both physical and virtual interfaces, including their physical port, redundant port, aggregation port and VLAN, and reports logs if their state changes. Staring from 6.0.1, FortiWeb no longer monitors the state changes of virtual interfaces.

Add log disk size limit in FortiWeb docker container

You can set log disk size limit. If the log disk usage exceeds the limit, logs will be deleted.

Upgrade instructions

Hardware & VM support

FortiWeb 6.0.1 supports:

- FortiWeb 100D
- FortiWeb 400C
- FortiWeb 400D
- FortiWeb 600D
- FortiWeb 1000D
- FortiWeb 1000E
- FortiWeb 2000E
- FortiWeb 3000C/3000CFsx
- FortiWeb 3000D/3000DFsx
- FortiWeb 3000E
- FortiWeb 3010E
- FortiWeb 4000C
- FortiWeb 4000D
- FortiWeb 4000E
- FortiWeb-VM

Repartitioning the hard disk

To upgrade from a version of FortiWeb previous to 5.5, you must first resize your FortiWeb operating system's disk.

In most cases, you'll have to install a special firmware image to repartition the disk. For details, see "To use the special firmware image to repartition the operating system's disk " on page 12.

For the following FortiWeb-VM tools, you cannot install the special firmware image to repartition the hard disk:

- Citrix XenServer
- Open-source Xen Project
- Microsoft Hyper-V
- KVM

For these platforms, to repartition the disk you must deploy a new virtual machine and restore the configuration and log data you backed up earlier. See "To repartition the operating system's disk without the special firmware image" on page 12.

Repartitioning affects the operating system's disk (USB/flash disk), not the hard disk. Existing data such as reports and event, traffic, and attack logs, which are on the hard disk, are not affected.

You can use this image to upgrade an HA cluster by following the same procedure you use for a regular firmware upgrade. For details, see "Updating firmware on an HA pair" in the *FortiWeb Administration Guide*:

http://docs.fortinet.com/fortiweb/admin-guides

To use the special firmware image to repartition the operating system's disk

1. Perform a complete backup of your FortiWeb configuration.

   Although the repartitioning firmware image automatically saves your FortiWeb configuration, Fortinet recommends that you also manually back it up. For details, see the *FortiWeb Administration Guide*:

   http://docs.fortinet.com/fortiweb/admin-guides

2. Go to the Fortinet Customer Service & Support website to download the special repartitioning firmware image from the FTP site:

   https://support.fortinet.com/

   Ensure that you download the correct image for your FortiWeb platform.

3. Follow one of the same procedures that you use to install or upgrade firmware using a standard image:

   - In the Web UI, go to **System > Status > Status**. Locate the **System Information** widget. Beside **Firmware Version**, click **[Update]**.
   - In the Web UI, go to **System > Maintenance > Backup & Restore**. Select the **Restore** option in **System Configuration**.
   - In the CLI, enter the `execute restore config` command.

   FortiWeb backs up the current configuration, resizes the hard drive partitions, and boots the system.

4. Continue with the instructions in "Upgrading from previous releases" on page 14.

To repartition the operating system's disk without the special firmware image

1. Perform a complete backup of your FortiWeb configuration. For details, see the *FortiWeb Administration Guide*:

   http://docs.fortinet.com/fortiweb/admin-guides

2. Use the instructions for your hypervisor platform to detach the log disk from the VM:

   - "To detach the log disk from a Citrix XenServer VM" on page 13
   - "To detach the log disk from a Microsoft Hyper-V VM" on page 13
   - "To detach the log disk from a KVM VM" on page 13

3. Deploy a new FortiWeb 5.5 or later virtual machine on the same platform.

4. Use the instructions for your hypervisor platform to attach the log disk you detached earlier to the new VM:

- "To attach the log disk to a Citrix XenServer VM" on page 13
- "To attach the log disk to a Microsoft Hyper-V VM" on page 13
- "To attach the log disk to a KVM VM" on page 14

5. Restore the configuration you backed up earlier to the new VM.
6. When you are sure that the new VM is working properly with the required configuration and log data, delete the old VM.

To detach the log disk from a Citrix XenServer VM

1. In Citrix XenCenter, connect to the VM.
2. In the settings for the VM, on the Storage tab, select **Hard disk 2**, and then click **Properties**.
3. For **Description**, enter a new description, and then click **OK**.
4. Select **Hard disk 2** again, and then click **Detach**.
5. Click **Yes** to confirm the detach task.

To detach the log disk from a Microsoft Hyper-V VM

1. In the Hyper-V Manager, select the FortiWeb-VM in the list of machines, and then, under **Actions**, click **Settings**.
2. Select **Hard Drive (data.vhd)**, and then click **Remove**.
3. Click **Apply**.

To detach the log disk from a KVM VM

1. In Virtual Machine Manager, double-click the FortiWeb-VM in the list of machines.
2. Click **Show virtual hardware details** (the "i" button).
3. Click **VirtIO Disk 2**, and then click **Remove**.

To attach the log disk to a Citrix XenServer VM

1. In Citrix XenCenter, connect to the VM.
2. In the settings for the new, FortiWeb 5.5 or later VM, on the Storage tab, select **Hard disk 2**, and then click **Delete**.
3. Click **Yes** to confirm the deletion.
4. On the Storage tab, click **Attach Disk**.
5. Navigate to the hard disk you detached from the old VM to attach it.
6. Start your new virtual machine.

To attach the log disk to a Microsoft Hyper-V VM

1. In the Hyper-V Manager, select the new, FortiWeb 5.5 or later virtual machine in the list of machines, and then, under Actions, click **Settings**.
2. Select **Hard Drive (log.vhd)**, and then click **Browse**.

3. Browse to the hard drive you detached from the old virtual machine to select it.
4. Click **Apply**.
5. Start the new virtual machine.

To attach the log disk to a KVM VM

For KVM deployments, you remove an existing virtual disk from the new VM before you attach the disk detached from the original VM.

1. In Virtual Machine Manager, double-click the new, FortiWeb 5.5 or later VM in the list of machines.
2. Click **Show virtual hardware details** (the "i" button).
3. Click **VirtIO Disk 2**, and then click **Remove**.
4. Click **Add Hardware**.
5. Click **Storage**, select **Select managed or other existing storage**, and then click **Browse**.
6. Click **Browse Local**.
7. Navigate to the log disk file for the original machine to select it, and then click **Open**.
8. For **Device type**, select **Virtio disk**, for **Storage format**, select **qcow2**, and then click **Finish**.
9. Start the new virtual machine.

Image checksums

To verify the integrity of the firmware file, use a checksum tool to compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for software releases are available from Fortinet Customer Service & Support:

https://support.fortinet.com

To download the Customer Service & Support image checksum tool

After logging in to the website, in the menus at the top of the page, click **Download**, and then click **Firmware Image Checksums**.

Alternatively, near the bottom of the page, click the **Firmware Image Checksums** button. This button appears only if one or more of your devices has a current support contract. In the **File Name** field, enter the firmware image file name including its extension, then click **Get Checksum Code**.

Upgrading from previous releases

- To upgrade from a version of FortiWeb previous to 5.5, you must first resize your FortiWeb hard disk partitions. See "Repartitioning the hard disk" on page 11.

- If you upgrade from a version of FortiWeb previous to 5.5.4, the upgrade process deletes any HTTP content routing policies that match X509 certificate content. You can re-create these policies using the new, enhanced X509 certificate settings.
- If you upgrade from a version of FortiWeb previous to 5.3.6, the upgrade process deletes any V-zone IP addresses, which are no longer required. This operation has no impact on routing or connectivity after the upgrade.
- If you upgrade from a version of FortiWeb previous to 5.3.4 and your server policy configuration includes settings that customize an attack blocking or server unavailable error page, the upgrade deletes these server-based settings. The functionality is replaced by the global, default FortiWeb pages.
- If you upgrade from 6.0, or downgrade from 6.0.1 to 6.0, the machine learning data will be cleared.

Note: To upgrade from 4.0 MR4, Patch x or earlier, please contact Fortinet Technical Support.

To upgrade from FortiWeb 5.5.x or later releases

Upgrade to FortiWeb 6.0.1 directly.

To upgrade from FortiWeb 5.4.x or FortiWeb 5.3.x

Upgrade to FortiWeb 6.0.1 directly after completing the hard disk repartitioning process.

If you are upgrading FortiWeb-VM on a hypervisor other than VMware vSphere, see "FortiWeb-VM license validation after upgrade from pre-5.4 version" on page 16.

To upgrade from a version previous to FortiWeb 5.3

FWB5.3.exe is a Microsoft Windows executable script that automatically migrates your FortiWeb 5.2.x configuration settings to a 5.3.x configuration.

1. If your version is 5.0.x or 5.1.x, upgrade to FortiWeb 5.2.x.
2. Use **System > Maintenance > Backup & Restore** to back up your FortiWeb configuration. Fortinet recommends that you use the **Backup entire** configuration option.

   Note: If you forget to back up the configuration before you upgrade to FortiWeb 5.3, you can use the **Boot into alternate firmware** option to downgrade to the previous version, and then backup its configuration. For details, see the *FortiWeb Administration Guide*:

   http://docs.fortinet.com/fortiweb/admin-guides
3. To obtain the upgrade script, log in to the Fortinet Customer Service & Support website:

   https://support.fortinet.com

   In the menus at the top of the page, click **Download**, and then click **Firmware Images**.
4. For product, select **FortiWeb**. Then, on the Download tab, navigate to the following folder:

   `/FortiWeb/v5.00/5.3/Upgrade_script/`
5. Download the .zip compressed archive (for example, `FWB5.3Upgrade_v1.9.zip`) to a location you can access from your Windows PC.
6. In Windows, extract the .zip archive's contents, and then use a command line interface to execute the upgrade script.

For example, in the directory where the file `FWB5.3Upgrade.exe` and your backup configuration file are located, execute the following command:

```
FWB5.3Upgrade.exe -i YOUR_CONFIG_NAME.conf -o 5.3_new.conf
```

The script removes the Domain Server, Physical Server, Server Farm, Content Routing policy configurations and generates a new configuration file named `5.3_new.conf`.

7. Resize your FortiWeb hard disk partitions. See "Repartitioning the hard disk" on page 11.
8. Upgrade to FortiWeb 6.0.1.
9. Use **System > Maintenance > Backup & Restore** to restore the configuration file you created using the script (for example, `5.3_new.conf`).

   If you upgrade from a previous version of FortiWeb and your server policy configuration includes settings that customize an attack blocking or server unavailable error page, the upgrade deletes these server-based settings. The functionality is replaced by the global, default FortiWeb pages.

Upgrading an HA cluster

If the HA cluster is running FortiWeb 4.0 MR4 or later, the HA cluster upgrade is streamlined. When you upgrade the active appliance, it automatically upgrades any standby appliance(s), too; no manual intervention is required to upgrade the other appliance(s). This includes upgrading using the special hard disk repartitioning firmware image for upgrading to 5.5 or later from earlier releases.

If the HA cluster is running FortiWeb 4.0 MR3 Patch x or earlier, contact Fortinet Technical Support for assistance.

Downgrading to a previous release

When you downgrade your FortiWeb 6.0.1 to version 5.1 or 5.0, the basic configuration for your appliance's connections to the network (e.g., IP address and route configuration) is preserved.

If you downgrade from 6.0.1 to 6.0, the machine learning database will be cleared.

FortiWeb-VM license validation after upgrade from pre-5.4 version

On some virtual machine deployments, upgrading FortiWeb-VM from a version previous to 5.4 changes the virtual machine's universal unique identifier (UUID). Because of this change, the first time you upload your existing FortiWeb-VM license, the FortiGuard Distribution Network (FDN) server reports that it is invalid.

To solve this problem, after you have uploaded the license, wait 90 minutes, and then upload the license again.

This issue does not affect FortiWeb-VM deployed on a VMware vSphere hypervisor.

Resolved issues

This section lists issues that have been fixed in version 6.0.1. For inquires about a particular bug, please contact Fortinet Customer Service & Support:

https://support.fortinet.com

Bug ID	Description
0508317	FTP scheduled dialy backup does not work if FTP passowrd contains special characters.
0503628	When **Session Ticket Reuse** is enabled, memory leak problem may occur.
0503364	FortiWeb does not work well in HTTP2 to HTTP2 scene.
0501080	When a same TCP traffic passes through two Vzones, HTTP traffic goes down after **Server Policy** is enabled.
0500386	No parse happens when no boundary is available in a multi-part request, which causes all WAF features are bypassed.
0498780	The cluster lost some configurations on its own.
0497251	`"cookie-security"` and `"allow-time"` are not automatically generated after the configuration change, which makes the master unit miss configuration and the slave unit keep reloading.
0496274	When running `"diagnose debug sslhardwarestatus show"`, the diagnose check result output for intel engine is missing.
0495644	HTTP parser does not support PATCH method, so HPC regards this method invalid .
0494287	Certificate name fails to be correctly imported due to white space after FortiWeb version upgraded to 5.9.1.
0495171	Machine Learning: In testing mode, the learning mode can not be refreshed.
0492847	Machine Learning: After the sample module is finished, the existing module is triggered to drop, with new attack modules generated.
0492628	The .txt and .xps files are not supported in **File Security Rule** list.
0491960	Aggregate interfaces go down on the slave unit when the signature exception is added on the master unit.
0491867	Machine Learning: Machine Learning needs to be enabled by default on **Other Log Settings** page.

Bug ID	Description
0488811	The HSM certificate could not be restored using the "`restore cert-config`" command.
0480965	Brute force login "Exchange 2013" in inline/offline profile is lost after FortiWeb version upgraded to 5.8.5 or higher.
0480895	Disabling **Recursive URL Decoding** of FortiWeb by default may cause WAF bypass.
0415766	Alert emails were sent whenever they were triggered instead of at the interval set in email policy.

Known issues

This section lists known issues in version 6.0.1, but may not be a complete list. For inquires about a particular bug, please contact Fortinet Customer Service & Support:

https://support.fortinet.com

Bug ID	Description
0511242	hasync CPU usage reaches up to 100% on one core randomly.
0509322	While executing FortiWeb reboot, MySQL errors occasionally appear on the CLI Console.
0507225	Importing/exporting machine learning data in policy level changes the order of domains.
0505966	Upload a WSDL file and modify the webservice, this triggers the reloading failure; the WSDL detection function does not work.
0505663	On FortiWeb 1000D platform, the master console has no response and reboot fails on both CLI and GUI.
0504105	HTTPS has a lot of zombie processes, and FortiWeb can not be accessed via the management port.
0503587	Machine Learning: CLI crashes when domain-name is added in Machine Learning.
0503300	Machine Learning: Shellcode detection function does not work well.
0502898	The error message "`undefined`" appears when the user logs into WAF.
0502506	Application confd sometimes crashes when saving the WAF configuration.
0501451	Machine Learning: When running "`execute db rebuild`", all the MySQL database is lost.
0501154	When running "`diag sys ha confd_status`", it shows the slave unit is in initial status.
0494366	tlog and alog logs have errors when the cookie key value is larger than 512 K.
0483785	The SFP Transreciever on Fortiweb Finisar FTLF8519P3BNL does not come up on FortiWeb 600D.